ABB DOC ID: 3ADR010465
REVISION: B
DATE: 2020-10-15

CYBER SECURITY ADVISORY

Automation Builder 2.2 (and before), Drive Application Builder 1.0

ABBVU-MODR-3ADR010465

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

Affected Products

The following products are affected by this vulnerability:

- All Automation Builder versions prior V2.3.0
  (only when using for programming AC500 V3 PLC or IEC61131 programmable Drives)
- Drive Application Builder V1.0.0

This applies to both the 32-bit and 64-bit variants.

Vulnerability ID

ABB ID: ABBVU-MODR-3ADR010465

Summary

ABB is aware of public reports of a vulnerability in the product versions listed above.

This issue will be fixed by

- Version 2.3.0 of Automation Builder. The release of this version is expected for end of Q1 2020
- Version 1.1.0 of Drive Application Builder. The release of this version is expected for end of 2019

An attacker who successfully exploited this vulnerability could insert and run arbitrary JavaScript and/or ActiveX code.

Update (2020-10-15):

Released versions of both tools including the fixes for this vulnerability are available for download from the related ABB websites:

- Automation Builder version 2.3.0: https://new.abb.com/plc/automationbuilder/platform/software
- Drive Application Builder version 1.1.0: https://new.abb.com/drives/software-tools/drive-application-programming

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

CVSS v3 Base Score: 8.6 (High)

CVSS v3 Vector: AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

CVSS v3 Link: https://www.first.org/cvss/calculator/3.0

Recommended immediate actions

ABB is currently investigating this vulnerability in order to provide adequate protection to customers.

Until a correction is available, ABB strongly recommends to only install libraries from trustworthy sources. It is also advised to enable strict security settings in web browser to limit execution of harmful JavaScript and/or ActiveX components.

Update (2020-10-15):

It is highly recommended to update to the latest version of Automation Builder or Drive Application Builder to close the vulnerability.

Vulnerability Details

Documentation is an elementary part of IEC 61131 libraries. In addition to the usually chosen straight representation the documentation can also be enriched with active contents. Since the affected tools try to display these without checking the validity, malicious contents of manipulated libraries may also be displayed or executed.

Mitigating Factors

Although ABB provides functionality testing on the products and updates that we release, you should institute your own testing program for any product updates or other major system updates (to include but not limited to code changes, configuration file changes, third party software updates or patches, hardware exchanges, etc.) to ensure that the security measures that you have implemented have not been compromised and system functionality in your environment is as expected. This also applies to the operating system. Security measures (such as but not limited to the installation of latest patches, installation of firewalls, application of authentication measures, installation of anti-virus programs, etc.) are in your responsibility. You have to be aware that operating systems provide a considerable number of open ports that should be monitored carefully for any threats.

Workarounds

ABB has currently found no workaround for this vulnerability. Therefore, you should only install and use IEC 61131 libraries from trustworthy sources.

Update (2020-10-15):

The issue has been fixed with Automation Builder version 2.3.0 and Drive Application Builder 1.1.0, which are available for download from the related ABB websites:

- Automation Builder version 2.3.0: https://new.abb.com/plc/automationbuilder/platform/software
- Drive Application Builder version 1.1.0: https://new.abb.com/drives/software-tools/drive-application-programming

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could insert and run arbitrary JavaScript and/or ActiveX code in an affected system.

What causes the vulnerability?

The vulnerability is caused by active components in IEC 61131-3 library documentation. These active components are displayed by the development environment without checking for validity.

What is the affected product?

The affected tools are IEC 61131-3 programming tools for the industrial controllers – Automation Builder and Drive Application Builder.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could insert and run arbitrary JavaScript and/or ActiveX code on the development PC.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by manipulating signed compiled libraries, e.g. by adding malicious JavaScript code to the documentation. This would require that the attacker has access to the libraries and can exchange them without notice. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

This vulnerability could be exploited by or with the help of local users. Libraries should only be installed from trustworthy sources. Recommended practices include limiting access to both development and control system by physical means, operating system features, etc. and protecting both development and control system by using up to date virus detecting solutions.

What does the update do?

After applying the planned software update, JavaScript included in the library documentation is only executed, if the library was correctly signed with a valid certificate.

When this security advisory was issued, had this vulnerability been publicly disclosed?

Yes, this vulnerability has been publicly disclosed by 3S-Smart Software Solutions GmbH.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

Acknowledgements

ABB thanks the following for working with us to help protect customers:

Heinz Füglister of WRH Walter Reist Holding AG for reporting this vulnerability following coordinated disclosure.

Support

For additional information and support please contact your local ABB service organization. For contact information, see https://new.abb.com/contact-centers.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.